IN THE CLAIMS:

Please cancel claims 1-10 and add new claims 11-20 in lieu thereof.

Claims 1-10 (canceled).

11. (new)   Method of encryption and decryption carried out by a plurality of encryption/decryption modules arranged in series, wherein a encryption/decryption module, different from the first module, starts encryption/decryption operations as soon as said module receives a part of the results of encryption/decryption operations from the immediately preceding encryption/decryption module.

12. (new)   Method according to Claim 11, wherein a decryption module, different from the first module, starts decryption operations as soon as said module receives a part of the results of decryption operations from the immediately preceding decryption module.

13. (new)   Method according to Claim 11, wherein an encryption module, different from the first module, starts encryption operations as soon as said module receives a part of the results of encryption operations from the immediately preceding encryption module.

14. (new)   Method according to Claim 11, carried out by three modules wherein the central module operates with a secret symmetric key.

15. (new)   Method according to claim 14, wherein the first module and the last module in respect of encryption and in reversed order the last module and the first module in respect of decryption operate with an algorithm using asymmetric keys including a private key and a public key.

16. (new)   Method according to claim 15, wherein the first module and the last module use the private key for encryption and the public key for decryption.

17. (new)   Method according to claim 16, wherein the first module and the last module use the same set of private and public keys.

18. (new)   Method according to Claim 16, wherein the first module and the last module use a different set of private and public keys.

19. (new)   Method according to Claim 15, wherein, the last module uses the public key during encryption and the first module uses the private key during decryption.

20. (new)   Method according to Claim 11, carried out by three encryption/decryption modules, wherein all three modules operate with asymmetric keys.